CHAPTER 1

Security Overview

Cisco Connected Grid OS software (hereafter referred to as Cisco CG-OS software) on the Cisco 1000 Series Connected Grid Routers (hereafter referred to as Cisco CG-OS router) supports security features that can protect your network against degradation or failure. These features can also protect against data loss or compromise resulting from intentional attacks and from unintended but damaging mistakes by network users.

This chapter includes the following sections:

- Authentication, Authorization, and Accounting, page 1-1
- RADIUS and TACACS+ Security Protocols, page 1-2
- SSHv2 and Telnet, page 1-2
- PKI, page 1-3
- User Accounts and Roles, page 1-3
- IKEv2 and IPSec, page 1-3
- IP ACLs, page 1-3

Authentication, Authorization, and Accounting

Authentication, authorization, and accounting (AAA) is an architectural framework for configuring a set of three independent security functions in a consistent, modular manner.

- Authentication—Provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol that you select, encryption. Authentication is the process of identifying a user before that user is allowed access to the network and network services. Configuring AAA authentication involves defining a named list of authentication methods and then applying that list to various interfaces.
- Authorization—Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights, with the appropriate user. AAA authorization works by assembling a set of attributes that describe what the user is authorized to perform. These attributes are compared with the information contained in a database for a given user, and the result is returned to AAA to determine the user’s actual capabilities and restrictions.
- Accounting—Provides the method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes. Accounting enables you to track the services that users are accessing, as well as the amount of network resources that they are consuming.

Note You can configure authentication outside of AAA. However, you must configure AAA if you want to use RADIUS or TACACS+, or if you want to configure a backup authentication method.

Related Topics

Chapter 4, "Configuring AAA"

RADIUS and TACACS+ Security Protocols

AAA uses security protocols to administer its security functions. When a router or access server is acting as a network access server, AAA is the means through which you establish communication between your network access server and your RADIUS or TACACS+ security server.

The chapters in this guide describe how to configure the following security server protocols:

- RADIUS—A distributed client/server system that allows you to secure networks against unauthorized access. In the Cisco implementation, RADIUS clients run on the Cisco CG-OS router and send authentication and accounting requests to a central RADIUS server that contains all user-authentication and network-service access information.
- TACACS+—A security application implemented through AAA that provides a centralized validation of users who are attempting to gain access to a router or network access server. TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, on a UNIX or Windows NT workstation. TACACS+ provides for separate and modular authentication, authorization, and accounting facilities. TACACS+ specifically requires Command Authorization and Configuration Authorization for Device Administration to the router.

Related Topics

Chapter 2, "Configuring RADIUS"

Chapter 3, "Configuring TACACS+"

SSHv2 and Telnet

You can use the Secure Shell version 2 (SSHv2) server to enable an SSHv2 client to make a secure, encrypted connection to the Cisco CG-OS router. SSHv2 uses strong encryption for authentication.

- The SSHv2 server in Cisco CG-OS software is interoperable with publicly and commercially available SSHv2 clients.
- The SSHv2 client in Cisco CG-OS software works with publicly and commercially available SSHv2 servers.

The Telnet protocol enables TCP/IP connections to a host. Telnet allows a user at one site to establish a TCP connection to a login server at another site and then passes the keystrokes from one device to the other. Telnet can accept either an IP address or a domain name as the remote device address.

Related Topics

Chapter 5, "Configuring SSHv2 and Telnet"

PKI

The Public Key Infrastructure (PKI) allows the Cisco CG-OS router to obtain and use digital certificates for secure communication in the network and provides manageability and scalability for applications, such as SSHv2, that support digital certificates.

Related Topics

Chapter 6, "Configuring PKI"

User Accounts and Roles

You can create and manage user accounts and assign roles that limit access to operations on the Cisco CG-OS router. This definition and assignment process is knows as role-based access control (RBAC).

Related Topics

Chapter 7, "Configuring User Accounts and RBAC"

IKEv2 and IPSec

Internet Key Exchange version 2 (IKEv2) and Cisco IP Security (IPSec) allow configuration of secure communications between a source (Cisco CG-OS router) and destination router over a virtual tunnel.

Related Topics

Chapter 8, "Configuring IKEv2 and IPSec"

IP ACLs

IP ACLs are ordered sets of rules that you can use to filter traffic based on IPv4 information in the Layer 3 header of packets. Each rule specifies a set of conditions that a packet must satisfy to match the rule. When Cisco CG-OS software determines that an IP ACL applies to a packet, it tests the packet against the conditions of all rules. The first match determines whether a packet is permitted or denied, or if there is no match, Cisco CG-OS software applies the applicable default rule. Cisco CG-OS software continues processing packets that are permitted and drops packets that are denied.

Related Topics

Chapter 9, "Configuring IP ACLs"

Control-Plane Policing

To prevent the Cisco CG-OS router from Denial of Service (DoS) attacks, the system employs control-plane policing (CoPP or CPP). CoPP increases security on the router by protecting the system from unnecessary or DoS traffic and gives priority to important control-plane and management traffic.

Related Topics

Chapter 10, "Configuring Control-Plane Policing"

Zero Touch Configuration

Zero Touch Deployment is an ease-of-use feature that automatically registers (enrolls) and distributes X.509 certificates and provisioning information over secure connections within a connected grid network.

Related Topics

Chapter 11, "Zero Touch Deployment"